

REMARKS

Applicant respectfully requests further examination and reconsideration in view of the arguments set forth fully below. Claims 1-43 were previously pending in this Application. Within the Office Action, Claims 1-43 have been rejected. By the above amendments, Claims 10 and 36 have been amended. Accordingly, Claims 1-43 are now pending in the application.

Rejections Under 35 U.S.C. § 102

Within the Office Action, Claims 1-43 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0010467 to Hori et al. (hereinafter “Hori”). The Applicant respectfully disagrees.

Hori teaches a content data storage system including a memory card having a memory to store encrypted content data, a license hold unit to store license information, a plurality of authentication data, each storing authentication data that are authenticated by a plurality of public authentication keys and a switch to selectively provide the data from the plurality of authentication data hold units outside of the recording apparatus according to a request external to the memory card. [Hori, Abstract] Hori teaches that an authentication server 12 challenges the authenticity of the user’s cellular phone and memory card establishing access for distribution of music data. [Hori, ¶ 0063] Hori further teaches that in response to a distribution request, license server 10 verifies the authenticity of the user’s memory card through authentication server 12, and distributes encrypted content data and license thereof corresponding to the music request to the user’s cellular phone. [Hori, ¶ 0064, Figure 1] Hori also teaches restricting the number of accesses to the memory card. [Hori, ¶ 0089] However, the number of accesses to the memory card is not the same as or similar to determining a level of access. Hori does not teach that the authentication data includes a predetermined level of content access. Hori teaches challenging the authenticity of the user’s device to establish access, not to determine a level of access. Hori further does not teach determining the predetermined level of content access. Furthermore, Hori does not teach the authentication data preinstalled on the memory device.

In contrast to the teachings of Hori, the system for authentication downloading of the presently claimed invention, utilizes a removable memory having a set of authentication data that includes a predetermined level of content access. A handheld electronic device includes an interface to connect to the Internet when the removable memory is inserted into the handheld electronic device and a connection is formed with a server, using the set of authentication data, the server is able to authenticate the removable memory automatically without the user

interfacing personally with the server. The server authenticates downloading to the removable memory in the handheld electronic device by reading the set of authentication data on the removable memory, and downloading the desired content to the removable memory. Removable memory is issued to the user having a pre-assigned set of authentication data tailored to the needs of the user and the authentication level desired by the user. [Present Specification, page 5, lines 6-9] As an example, in this embodiment, free content results in a free removable memory, while content normally sold for a fee results in a fee for the removable memory. [Present Specification, page 5, lines 9-12] By using a subscription identification number, a server is able to identify what content the user is authorized to download from the server. [Present Specification, page 5, lines 13-19] As described above, Hori does not teach that the authentication data includes a predetermined level of content access. As further described above, Hori teaches challenging the authenticity of the user's device to establish access, not to determine a level of access. As also described above, Hori does not teach determining the predetermined level of content access.

It is stated within the Response to Arguments section of the Office Action, that Hori teaches determining a predetermined level of content access. The Applicant respectfully disagrees. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to *determine a level of access*. Per Hori's teachings, establishing access is *all or nothing*. In contrast to the *all or nothing* teachings of Hori, the system for authentication downloading of the presently claimed invention, utilizes a removable memory having a set of authentication data that includes a *predetermined level of content access*.

Furthermore, Hori also teaches:

Information to control the operation of the apparatus constituting the system, i.e. cellular phone 100 which is a content reproduction circuit and memory card 110, includes purchase condition information AC transmitted from cellular phone 100 to distribution server 30 when a user purchases a content decryption key or the like for the purpose of specifying the purchase condition, access restriction information AC1 indicating restriction and the like as to the number of accesses to memory card 110... [Hori, ¶89]

Thus, Hori specifically teaches "the number of accesses to [the] memory card" are restricted based on the restriction information. Thus, Hori restricts the number of accesses but not the level of content access. Contrastingly, the present invention is directed to "[t]he set of authentication data will determine how much, if any of the content on the server 150 is available to the user to download." [Present Specification, page 6, lines 20-21] Thus, Hori still does not teach determining the level of content access.

Furthermore, the present invention is directed to a removable memory where the manufacturer stores the authentication data on the removable memory. In some embodiments, the manufacturer of the removable memory stores the authentication data before the removable memory is sold or provided to a user. [Present Specification, page 6, lines 28-30] Contrastingly, Hori does not teach the authentication data is preinstalled on the removable memory.

Moreover, the present invention is directed to the predetermined level of content access determines how much of the content on the server is available for download. [Present Specification, page 6, lines 20-21] However, Hori does not teach the predetermined level of content access determines how much of the content on the server is available for download.

The independent Claim 1 is directed to a method of downloading content from a server to an electronic device. The method of Claim 1 comprises storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, accessing the server with the electronic device, authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access and downloading the content from the server to the removable memory according to the predetermined level of content access. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to determine a *level of access*. As further described above, Hori does not teach that the authentication data includes a *predetermined level of content access*. For at least these reasons, the independent Claim 1 is allowable over the teachings of Hori.

Claims 2-9 are all dependent on the independent Claim 1. As described above, the independent Claim 1 is allowable over the teachings of Hori. Accordingly, Claims 2-9 are all also allowable as being dependent on an allowable base claim.

Furthermore, the dependent Claim 4 is directed to time stamping the authentication data, such that the predetermined level of content access is available for a predetermined amount of time. While Hori teaches time elapses for secret keys and public keys as well as inhibiting usage of certificate keys after an elapse of a predetermined period of time [Hori, ¶99, ¶100 and ¶115], Hori clearly does not teach time stamping the authentication data, such that the predetermined level of content access is available for a predetermined amount of time. For at least these additional reasons, the dependent Claim 4 is allowable over the teachings of Hori.

The independent Claim 10 is directed to a system for downloading content from a server to an electronic device. The system of Claim 10 comprises means for storing authentication data on a removable memory, wherein the authentication data includes a predetermined level of content access, further wherein the authentication data is preinstalled on the removable memory,

means for receiving the removable memory in the electronic device, means for accessing the server with the electronic device, means for authenticating the removable memory by reading the authentication data from the removable memory to determine the predetermined level of content access and means for downloading the content from the server to the removable memory according to the predetermined level of content access. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to determine a *level of access*. As further described above, Hori does not teach that the authentication data includes a *predetermined level of content access*. Furthermore, Hori does not teach wherein the authentication data is preinstalled on the removable memory. For at least these reasons, the independent Claim 10 is allowable over the teachings of Hori.

Claims 11-18 are all dependent on the independent Claim 10. As described above, the independent Claim 10 is allowable over the teachings of Hori. Accordingly, Claims 11-18 are all also allowable as being dependent on an allowable base claim.

Furthermore, the dependent Claim 13 is directed to wherein the authentication data also includes a time stamp, such that the predetermined level of content access is available for a predetermined amount of time. While Hori teaches time elapses for secret keys and public keys as well as inhibiting usage of certificate keys after an elapse of a predetermined period of time [Hori, ¶99, ¶100 and ¶115], Hori clearly does not teach wherein the authentication data also includes a time stamp, such that the predetermined level of content access is available for a predetermined amount of time. For at least these additional reasons, the dependent Claim 13 is allowable over the teachings of Hori.

The independent Claim 19 is directed to a system for downloading content. The system of Claim 19 comprises a removable memory, the removable memory including authentication data, the authentication data including a predetermined level of content access, an electronic device configured to receive the removable memory and a server, wherein when the electronic device accesses the server, the removable memory is authenticated by reading the authentication data from the removable memory and determining the predetermined level of content access, and further wherein once authenticated, content according to the predetermined level of content access is downloaded from the server to the electronic device. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to determine a *level of access*. As further described above, Hori does not teach that the authentication data includes a *predetermined level of content access*. For at least these reasons, the independent Claim 19 is allowable over the teachings of Hori.

Claims 20-27 are all dependent on the independent Claim 19. As described above, the independent Claim 19 is allowable over the teachings of Hori. Accordingly, Claims 20-27 are all also allowable as being dependent on an allowable base claim.

Furthermore, the dependent Claim 22 is directed to wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. While Hori teaches time elapses for secret keys and public keys as well as inhibiting usage of certificate keys after an elapse of a predetermined period of time [Hori, ¶99, ¶100 and ¶115], Hori clearly does not teach wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. For at least these additional reasons, the dependent Claim 22 is allowable over the teachings of Hori.

The independent Claim 28 is directed to an electronic device for downloading. The electronic device of Claim 28 comprises a memory slot configured to receive a removable memory, wherein the removable memory includes authentication data, the authentication data including a predetermined level of content access, and a communications interface configured for coupling to a server, wherein when the electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access, further wherein content according to the predetermined level of content access is downloaded. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to determine a *level of access*. As further described above, Hori does not teach that the authentication data includes a *predetermined level of content access*. For at least these reasons, the independent Claim 28 is allowable over the teachings of Hori.

Claims 29-35 are all dependent on the independent Claim 28. As described above, the independent Claim 28 is allowable over the teachings of Hori. Accordingly, Claims 29-35 are all also allowable as being dependent on an allowable base claim.

Furthermore, the dependent Claim 31 is directed to wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. While Hori teaches time elapses for secret keys and public keys as well as inhibiting usage of certificate keys after an elapse of a predetermined period of time [Hori, ¶99, ¶100 and ¶115], Hori clearly does not teach wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. For at least these additional reasons, the dependent Claim 31 is allowable over the teachings of Hori.

The independent Claim 36 is directed to a removable memory for downloading. The removable memory of Claim 36 comprises authentication data, the authentication data including a predetermined level of content access and a communications interface configured for coupling to a server, wherein when an electronic device accesses the server through the communications interface, the removable memory is authenticated by reading the authentication data from the removable memory to determine the predetermined level of content access, further wherein the electronic device includes a memory slot configured to receive the removable memory, and further wherein content according to the predetermined level of content access is downloaded, further wherein the predetermined level of content access determines how much of the content on the server is available for download. As described above, Hori teaches challenging the authenticity of the user's device to *establish access*, not to determine a *level of access*. As further described above, Hori does not teach that the authentication data includes a *predetermined level of content access*. Furthermore, Hori does not teach the predetermined level of content access determines how much of the content on the server is available for download. For at least these reasons, the independent Claim 36 is allowable over the teachings of Hori.

Claims 37-43 are all dependent on the independent Claim 36. As described above, the independent Claim 36 is allowable over the teachings of Hori. Accordingly, Claims 37-43 are all also allowable as being dependent on an allowable base claim.

Furthermore, the dependent Claim 39 is directed to wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. While Hori teaches time elapses for secret keys and public keys as well as inhibiting usage of certificate keys after an elapse of a predetermined period of time [Hori, ¶99, ¶100 and ¶115], Hori clearly does not teach wherein the authentication data is time stamped, such that the predetermined level of content access is available for a predetermined amount of time. For at least these additional reasons, the dependent Claim 39 is allowable over the teachings of Hori.

For the reasons given above, the applicant respectfully submits that the claims are now in a condition for allowance, and allowance at an early date would be appreciated. Should the Examiner have any questions or comments, they are encouraged to call the undersigned at (408) 530-9700 to discuss the same so that any outstanding issues can be expeditiously resolved.

Respectfully submitted,
HAVERSTOCK & OWENS LLP

Dated: June 11, 2008

By: /Jonathan O. Owens/

Jonathan O. Owens
Reg. No. 37,902
Attorneys for Applicant(s)